

REMARKS

I. Status of Claims

The applicants have carefully considered the Office Action dated February 21, 2008, and the references cited therein. In the Office Action, claims 1-5 and 7-10 were rejected under 35 U.S.C. § 103(a) as being unpatentable over 3rd Generation Partnership Project, "Document 2: KASUMI Specification" Release 4, 2001-08-28 (DKS), and further in view of U.S. Patent No. 6,324,288 to Hoffman (Hoffman) and in view of "Parallel stream cipher for secure high-speed communications", 2001-07-09, by Hoonjae Lee (Lee)

II. Formalities

In the Office Action, the Examiner failed to acknowledge acceptance of the formal drawings. The applicants respectfully request that the Examiner acknowledge acceptance of the formal drawings.

III. Rejections under 35 U.S.C. § 103(a)

With respect to independent claims 1 and 8, the applicants disagree with the Examiner's allegations. In particular, there is nothing in the alleged combination of DKS and Lee that discloses or teaches a method for performing a first-round of encryption by encrypting the received first and second sub-bit streams with predetermined first encryption codes an odd number of times, and outputting the second ciphertext bit stream encrypted again with a predetermined time delay right after the first ciphertext bit streams of length n are output; generating a first operated ciphertext bit stream by performing a logical exclusive-OR operation on the first ciphertext bit stream and the third sub-bit stream at the same time of performing encryption of the second ciphertext bit stream; generating a second operated ciphertext bit stream by performing a logical exclusive-OR operation on the second ciphertext bit stream and the fourth sub-bit stream; and performing a second-round of encryption by

encrypting the received first operated ciphertext bit stream and the second operated ciphertext, comprising the predetermined time delay, with predetermined second encryption codes an odd number of times, and concurrently outputting the third and fourth ciphertext bit streams of length n after encryption the first operated ciphertext bit stream again with predetermined second encryption codes.

To exemplify the recitations of independent claims 1 and 8, the applicants direct the Examiner's attention to FIG. 5 of the present patent application. In FIG. 5, a first-round of encryption (501) is performed by encrypting the received first and second sub-bit streams (L_0 , R_0 , respectively) with predetermined first encryption codes ($KO_{1,1}$, $KO_{1,2}$, respectively) an odd number of times, and the second ciphertext bit stream (R_{3D}), which is encrypted again ($KI_{1,2}$), is output with a predetermined time delay (D_7) right after the first ciphertext bit stream (R_3) of length n are output.

DKS discloses a first round of encryption where the integer i constitutes the round i th round function of KASUMI. A 64-bit input I is divided into two 32-bit strings L_0 and R_0 . The function FL1 receives the 32-bit L_0 and a 32-bit subkey KL_1 . The subkey is split into two 16-bit subkeys, $KL_{i,1}$ and $KL_{i,2}$, and the input data I is split into two 16-bit halves, L and R where $I=L||R$. The 32-bit output value is $(L||R)$. See Figure 4 and sections 3.2 and 4.2 on page 11. Function FO1 receives the output of FL1, which comprises a 32-bit string L_0 and two sets of subkeys, a 48-bit subkey KO_1 and a 48-bit subkey KI_1 . The 32-bit data input is split into two halves, L_0 and R_0 , where $I = L_0||R_0$. The 48-bit subkeys are subdivided into three 16-bit subkeys where $KO_i=KO_{i,1}||KO_{i,2}||KO_{i,3}$ and $KI_i=KI_{i,1}||KI_{i,2}||KI_{i,3}$. The 32-bit value $(L_3||R_3)$ is returned. See Figures 1 and 2 and section 4.3.

Further, there is nothing in DKS that discloses or teaches that the second sub-bit stream R_0 is encrypted with subkeys KL_1 , KO_1 , KI_1 in the first round of encryption (FL1, FO1). The second sub-bit stream R_0 of DKS is input to an exclusive-OR operation in the first

round. There is also nothing in DKS that discloses or teaches a second ciphertext bit stream because R_0 is not initially encrypted with subkeys and R_0 is not encrypted again with the subkeys. Moreover, there is nothing in DKS that discloses or teaches a second ciphertext bit stream being output **with a predetermined time delay**. Accordingly, DKS fails to disclose or teach a method for performing a first-round of encryption by encrypting the received first and second sub-bit streams with predetermined first encryption codes an odd number of times, and outputting the second ciphertext bit stream, which is encrypted again, with a predetermined time delay right after the first ciphertext bit streams of length n are output.

Also in FIG. 5 of the present application, a first operated ciphertext bit stream (R_4) is generated by performing a logical exclusive-OR operation on the first ciphertext bit stream (R_3) and the third sub-bit stream (R_0) at the same time of performing encryption of the second ciphertext bit stream (L_5).

DKS discloses in the first round, performing a logical exclusive-OR operation on the second 32-bit string R_0 and the output of FO1, which comprises a 32-bit value ($L_3||R_3$). There is nothing in DKS that discloses or teaches that a **third sub-bit stream** is used to perform a logical exclusive-OR operation. Instead, the second 32-bit string R_0 is used to perform a logical exclusive-OR operation with the output of FO1. Accordingly, DKS fails to disclose or teach a method for generating a first operated ciphertext bit stream.

Further in FIG. 5 of the present application, a second operating ciphertext bit stream (L_6) is generated by performing a logical exclusive-OR operation on the second ciphertext bit stream (L_5) and the fourth sub-bit stream (L_0).

DKS discloses in the first round, performing a logical exclusive-OR operation on the output of FO1, which comprises a 32-bit value ($L_3||R_3$). There is nothing in DKS that discloses or teaches a second ciphertext bit stream since the second ciphertext bit stream of

the present application is output with a **predetermined time delay**. Further, there is also nothing in DKS that discloses or teaches a **time delay**. Accordingly, DKS fails to disclose or teach a method for generating a second operated ciphertext bit stream.

Also in FIG. 5 of the present application, a second-round of encryption (502) is performed by encrypting the received first operated ciphertext bit stream (R_4) and the second operated ciphertext bit stream (L_6), comprising the predetermined time delay, with predetermined second encryption codes ($KO_{2,2}$, $KO_{2,3}$, respectively) an odd number of times, and concurrently outputting the third and fourth ciphertext bit streams of length n (L_8 , R_8 , respectively) after encrypting the first operated ciphertext bit stream again with predetermined second encryption codes.

DKS discloses a second round of encryption (FO2, FL2) in which function FO2 receives the output of the exclusive-OR operation, in the first round, performed on R_0 and the output of the function FO1. The function FO2 also receives two sets of subkeys, a 48-bit subkey KO_2 and a 48-bit subkey KI_2 . The function FL2 receives the output of the function FO2 and a 32-bit subkey KL_2 .

That is, DKS does not disclose or teach a first operated ciphertext bit stream and a second operated ciphertext bit stream, as discussed above. Moreover, there is nothing in DKS that discloses encrypting a first operated ciphertext bit stream and a second operated ciphertext bit stream **comprising a time delay**. DKS discloses encrypting the output of the exclusive-OR operation, in the first round, performed on R_0 and the output of the function FO1. Accordingly, DKS fails to disclose or teach performing a second-round of encryption by encrypting the received first operated ciphertext bit stream and the second operated ciphertext, comprising the predetermined time delay, with predetermined second encryption codes an odd number of times, and concurrently outputting the third and fourth ciphertext bit streams

of length n after encrypting the first operated ciphertext bit stream again with predetermined second encryption codes.

In rejecting claim 1, the Examiner admits that DKS does not explicitly disclose performing encryption of first and second ciphertext bit stream at the same time. To cure the deficiencies of DKS, the Examiner alleges that Lee discloses performing encryption of first and second ciphertext bit streams at the same time, by referencing pages 262-263 and section 2.3 of Lee, and asserting that Lee teaches this concept by identifying nonlinear functions to run those nonlinear function combined in parallel. According to the Examiner, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teachings of DKS by combining two nonlinear function (i.e., two FO units) as taught by Lee in order to optimize speed or faster processing.

The applicants respectfully disagree and submit that Lee does not cure the deficiencies of DKS. Lee discloses a parallel stream cipher that generates independent sequences from nonlinear combine functions via N LFSRs. Each (m) sequence enciphers from a plaintext block to a ciphertext block in parallel, which makes the proposed cipher m -times faster than a conventional stream cipher.

There is nothing in Lee that discloses or teaches a first operated ciphertext bit stream and second operated ciphertext bit stream, which comprises a time delay. In the present application, a first operated ciphertext bit stream is generated by performing a logical exclusive-OR operation on the first ciphertext bit stream and the third sub-bit stream at the same time of performing encryption of the second ciphertext bit stream, and a second operated ciphertext bit stream is generated by performing a logical exclusive-OR operation on the second ciphertext bit stream and the fourth sub-bit stream. Moreover there is nothing in Lee that discloses or teaches a third sub-bit stream and a fourth sub-bit stream. The encryption process of Lee is performed on m -bits shifted within a clock, which the m

feedback paths are independently XORed based on each combination of feedback taps. *See* section 2.2 on page 260. There is nothing in Lee that discloses or teaches a first ciphertext bit stream and a third sub-bit stream is XORed, and a second ciphertext bit stream and a fourth sub-bit stream is XORed.

Therefore, the Examiner has not provided any motivation for combining the references. The Examiner asserts that it would have been obvious to modify the teachings of DKS by combining two nonlinear functions (i.e., two FO units) as taught by Lee. The functions f_1, f_2, \dots, f_m are m -parallel nonlinear combine functions as a generalized model, which use m -bit memories and PS-LFSRs. The function FO of DKS uses a 48-bit subkey KO_i and a 48-bit subkey KI_i to encrypt data input I . Accordingly, the functions f_1, f_2, \dots, f_m of Lee are not analogous to the function FO of DKS. Accordingly the combination of Lee and DKS does not result in the recitations of the claims. Likewise, Campbell does not supply the at least above-noted deficiencies of DKS and Lee.


In view of the above, claims 1 and 8 would not have been obvious from any reasonable combination of DKS and Lee at least for reasons noted above. Therefore, the rejections of claims 1 and 8 and all dependents therefrom are in condition for allowance and the notice to that effect is respectfully requested.

IV. Conclusion

The applicants submit that the above arguments are fully responsive to the Office Action dated February 21, 2008 and respectfully request the asserted grounds of rejections be withdrawn based on such arguments. In view of the above, the applicants believe that all pending claims are in condition for allowance and notice to that effect is respectfully requested. Should the Examiner have any questions, the Examiner is encouraged to contact the undersigned at the telephone number indicated below.

Amendment filed June 19, 2008
Responding to Office Action mailed February 21, 2008
App. Serial No. 10/679,391

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Simon Booth', written over a horizontal line.

Simon Booth
Attorney of Record
Reg. No. 58,582

Roylance, Abrams, Berdo & Goodman, L.L.P.
1300 19th Street, N.W., Suite 600
Washington, D.C. 20036-2680
(202) 659-9076

Dated: June 19, 2008